

# Fractions and Decimals

Tom Davis

tomrdavis@earthlink.net

<http://www.geometer.org/mathcircles/fractions.pdf>

November 15, 2025

## 1 Introduction

If you divide 1 by 81, you will find that  $1/81 = .012345679012345679 \dots$ . The first time I did this, I was amazed—there was a beautiful pattern, but then instead of going “789”, it jumped directly from 7 to 9, and then started repeating. Is this a miracle? Are there any other cool patterns? Can we compose fractions with interesting expansions? Is there anything special about those sorts of fractions?

Some fractions come out even when expressed as a decimal:  $1/2 = 0.5$  and  $1/5 = 0.2$ , for example. Others repeat forever:  $1/3 = 0.3333 \dots$  or  $1/7 = .142857142857 \dots$ . Some only repeat after a while:  $1/6 = .16666 \dots$

Why do they repeat? Do decimals have to repeat? What is meant by  $1 = .9999 \dots$ ? How can you find the fraction corresponding to an infinite decimal or the decimal expansion of a given fraction? How much, if any, of this is caused by the fact that we work in base 10?

How do you convert a fraction to a decimal? A decimal to a fraction? What if the decimal is repeating?

These are the sorts of problems we’ll examine in this paper.

Appendix A contains a table of the properties of the decimal expansions of the fractions of the form  $1/n$  for  $n = 1$  to  $n = 900$ .

Some properties are easy, and some are difficult. In Appendices B, C, D and E are the definitions and simple properties of some number-theoretic concepts and functions that are used in the text.

## 2 What is a Decimal Number?

Almost everyone knows what a decimal number means, but let’s review it quickly anyway. Every decimal number has one of the digits from 0 through 9 in each of several positions. As you move from left to right, the digits represent smaller and smaller numbers.

For example, what is the meaning of the expression “134.526”? The digits to the left of the decimal point (“134” in this case) represent the size of the integer (whole-number) part of the number. Reading digits from the decimal point to the left, the first represents the “one’s” place, the next, the “ten’s” place, then the “hundred’s” place, and so on. We can rewrite the whole number 134 as:

$$1 \times 100 + 3 \times 10 + 4 \times 1,$$

or better, as:

$$1 \times 10^2 + 3 \times 10^1 + 4 \times 10^0.$$

The second expression is better, since we can see the progression of the exponents as we work through the digits. Thus, the original example “134.526” represents:

$$1 \times 100 + 3 \times 10 + 4 \times 1 + 5 \times \frac{1}{10} + 2 \times \frac{1}{100} + 6 \times \frac{1}{1000},$$

or better, as:

$$1 \times 10^2 + 3 \times 10^1 + 4 \times 10^0 + 5 \times 10^{-1} + 2 \times 10^{-2} + 6 \times 10^{-3}.$$

## 2.1 Non-Terminating Decimals

The explanation above is fine for decimals that terminate, but what does it mean when the decimal expansion goes on “forever”, as in  $1/3 = 0.333333\dots$ ? This is, in fact, probably the first infinite series that most people ever encounter, even if they don’t recognize it as an infinite series. The decimal expansion of  $1/3$  means this:

$$\frac{1}{3} = 3\left(\frac{1}{10}\right)^1 + 3\left(\frac{1}{10}\right)^2 + 3\left(\frac{1}{10}\right)^3 + 3\left(\frac{1}{10}\right)^4 + \dots = \sum_{i=1}^{\infty} 3\left(\frac{1}{10}\right)^i. \quad (1)$$

The sum above must continue *forever* before it is *exactly* equal to  $1/3$ . If you stop after any finite number of terms, it is not exact. Let us, in fact, look at the errors for a few approximations:

$$\begin{aligned} 1/3 - .3 &= 1/3 - 3/10 = 1/30 \\ 1/3 - .3333 &= 1/3 - 3333/10000 = 1/30000 \\ 1/3 - .3333333333 &= 1/3 - 3333333333/10000000000 = 1/30000000000. \end{aligned}$$

It is clear that the approximations are better and better, the last one above having an error of only one part in thirty billion, but no finite approximation is exact. For a proof that the infinite decimal expansion in Equation 1 is *exactly* equal to  $1/3$ , see section 4.

A mathematician would say that the limit of the sequence:

$$.3, .33, .333, .3333, .33333, .333333, \dots$$

is  $1/3$ . This means that given any error, no matter how small, after a certain point the terms in the sequence above will all be closer to  $1/3$  than that specified error.

In a sense, one reason that there are common misunderstandings about infinite decimal expansions of numbers is that to understand them completely, one needs to understand the mathematical concept of a limit, which is usually introduced in the introduction to calculus course. With that understanding, the fact that  $0.999\dots = 1$  becomes clear, as well as the fact that every decimal number that “is exact” in fact has two decimal expansions. For example,  $1/4 = 0.25 = 0.24999\dots$ , or  $0.123 = 0.12999\dots$ .

## 3 How to Convert Fractions to Decimals

To convert a fraction of the form  $i/j$  to a decimal, all you need to do is a long division where you write the numerator followed by a decimal point and as many zeroes as you want. For example, to convert the fraction  $7/27$  into a decimal, begin with the long division displayed below:

$$\begin{array}{r}
 .25925 \\
 27 \overline{) 7.00000} \\
 \underline{54} \phantom{00} \\
 160 \phantom{0} \\
 \underline{135} \phantom{0} \\
 250 \phantom{0} \\
 \underline{243} \phantom{0} \\
 70 \phantom{0} \\
 \underline{54} \phantom{0} \\
 160 \phantom{0} \\
 \underline{135} \phantom{0} \\
 25
 \end{array}$$

At each stage in the long division, the remainder will have to be less than 27, so in this case there are only 27 possible remainders: 0, 1, ..., 26. If the remainder were 27 or more, you could have divided at least one more 27 into it.

In the case above, the remainders are 16, 25, 7, 16, and 25. But once we are doing the division in the part of the fraction where all the decimals in the numerator are zero, if a remainder is repeated, the entire sequence of remainders will repeat from that point on, forever. In the case above, as soon as we hit the remainder of 16, the next one will have to be 25 and then the next one will have to be 7, and then 16, 25, 7, 16, and so on, forever. Thus, the infinite decimal expansion becomes:

$$7/27 = .259259259259\dots$$

Every fraction will eventually go into a cycle like this. The example above cycles all of its digits. Other fractions may have a non-repeating part followed by a part that repeats forever. For example, the fraction  $1/6 = .166666\dots$

It is also interesting to note that the repeating part of any decimal expansion of a fraction has to be shorter than the denominator. As we saw above, for example, if the denominator is 27, there are only 26 possible remainders in the long division: 1 through 26. A remainder of 0 means it came out even, and all the remainders have to be strictly less than 27.

In the two examples above it is pretty obvious from the "... " what part repeats, but if you wish to be mathematically precise, you can indicate the repeating part with a bar over the part that repeats. Hence:

$$\begin{aligned}
 7/27 &= .\overline{259} \\
 1/6 &= .\overline{16}
 \end{aligned}$$

It is interesting to make a table of the decimal expansions for the fractions with small denominators. Here's the list of the fractions of the form  $1/n$ :

1/2	.5	1/12	.08 $\bar{3}$	1/22	.04 $\bar{5}$
1/3	. $\bar{3}$	1/13	. $\overline{076923}$	1/23	. $\overline{0434782608695652173913}$
1/4	.25	1/14	. $\overline{0714285}$	1/24	.041 $\bar{6}$
1/5	.2	1/15	. $\overline{06}$	1/25	.04
1/6	.1 $\bar{6}$	1/16	.0625	1/26	. $\overline{0384615}$
1/7	. $\overline{142857}$	1/17	. $\overline{0588235294117647}$	1/27	. $\overline{037}$
1/8	.125	1/18	. $\overline{05}$	1/28	. $\overline{03571428}$
1/9	. $\bar{1}$	1/19	. $\overline{052631578947368421}$	1/29	. $\overline{0344827586206896551724137931}$
1/10	.1	1/20	.05	1/30	. $\overline{03}$
1/11	. $\overline{09}$	1/21	. $\overline{047619}$	1/31	. $\overline{032258064516129}$

There are some interesting patterns to note, even with such a small table. First, the decimals terminate (end with an infinite sequence of zeroes) exactly when the denominator is a multiple of a power of 2 and a power of 5, such as  $2 = 2^1$ ,  $4 = 2^2$ ,  $5 = 5^1$ ,  $8 = 2^3$ ,  $10 = 2^1 5^1$ ,  $16 = 2^4$  and  $20 = 2^2 5^1$ . If you want more data, Appendix A contains the cycle lengths for fractions with denominators up to 900.

Fractions with prime numbers as the denominator tend to have longer expansions, many of them having length  $p - 1$  where the denominator is the prime number  $p$ .

## 4 Converting Repeating Decimals to Fractions

Begin with the familiar expansion:

$$\frac{1}{3} = 3\left(\frac{1}{10}\right)^1 + 3\left(\frac{1}{10}\right)^2 + 3\left(\frac{1}{10}\right)^3 + 3\left(\frac{1}{10}\right)^4 + \dots = \sum_{i=1}^{\infty} 3\left(\frac{1}{10}\right)^i.$$

The example above (and *all* repeating decimals will be similar) is a geometric series. Every term after the first is just a constant multiple of the previous term. The first term in the expansion of  $1/3$  is  $3/10$  and each successive term is obtained by multiplying the previous term by  $1/10$ .

If the repeating part has more than one digit, the difference is that the multiplier is no longer  $1/10$ . For example, the number:

$$\overline{.345} = .345345345\dots = 345\left(\frac{1}{1000}\right) + 345\left(\frac{1}{1000}\right)^2 + 345\left(\frac{1}{1000}\right)^3 + \dots$$

The general form for a geometric series whose first term is  $a$  and whose ratio between terms is  $r$  is this:

$$S = a + ar + ar^2 + ar^3 + ar^4 + \dots = \sum_{i=0}^{\infty} ar^i. \quad (2)$$

if  $|r| < 1$  then the series converges. The usual trick to find the sum  $S$  is to multiply Equation 2 by  $r$  and then to subtract it from the original series to obtain:

$$\begin{aligned} S &= a + ar + ar^2 + ar^3 + ar^4 \dots \\ -rS &= -(ar + ar^2 + ar^3 + ar^4 + \dots) \\ \hline S - rS &= a. \end{aligned}$$

Thus  $S(1 - r) = a$ , or  $S = a/(1 - r)$ .

In the case of the fraction  $1/3$  above,  $a = 3/10$  and  $r = 1/10$  so:

$$S = \frac{3/10}{(1 - 1/10)} = \frac{3/10}{9/10} = \frac{3}{9} = \frac{1}{3}.$$

In the case of the decimal  $\overline{.345}$ , we have  $a = 345/1000$  and  $r = 1/1000$ , so:

$$S = \frac{345/1000}{1 - 1/1000} = \frac{345/1000}{999/1000} = \frac{345}{999} = \frac{115}{333}.$$

Exactly the same idea can be applied to decimals that repeat after an initial non-repeating part. For example, to show that the decimal  $0.166666\dots$  is  $1/6$ , notice that we have

$$.1666\dots = .1 + .0666\dots = \frac{1}{10} + \frac{6}{100} + \frac{6}{100}\left(\frac{1}{10}\right) + \frac{6}{100}\left(\frac{1}{10}\right)^2 + \frac{6}{100}\left(\frac{1}{10}\right)^3 + \dots.$$

Thus it is the sum of  $1/10$  and a geometric series with  $a = 6/100$  and  $r = 1/10$ :

$$.1666\dots = \frac{1}{10} + \frac{6/100}{1 - 1/10} = \frac{1}{10} + \frac{2}{30} = \frac{5}{30} = \frac{1}{6}.$$

A very similar trick can be used to convert any non-terminating decimal to a fraction. For example, what is the fractional form for

$$.345752375237523\dots = \overline{.3457523}?$$

The arithmetic is a bit ugly, but this is just:

$$\begin{aligned} \overline{.3457523} &= \frac{345}{1000} + \frac{7523}{10000000} + \frac{7523}{10000000}\left(\frac{1}{10000}\right)^1 \\ &\quad + \frac{7523}{10000000}\left(\frac{1}{10000}\right)^2 + \frac{7523}{10000000}\left(\frac{1}{10000}\right)^3 + \dots \\ &= \frac{345}{1000} + \frac{(7523/10000000)}{(1 - 1/10000)} = 1728589/4999500. \end{aligned}$$

You may have noticed that there is a trick that can be used with any decimal that repeats from the decimal point. To obtain the fraction, take the repeating part and divide it by a number with the same number of digits, but all of which are 9. For example, to convert  $\overline{.123}$  to a fraction, the repeating part is three digits long, so the fraction is  $123/999 = 41/333$ . Can you see why this always works?

## 5 Why is $.99999\dots = 1$ ?

Many people are disturbed by the fact that the repeating decimal  $.999\dots$  is equal to 1. According to our conversion trick, the repeating part is just 9, so the decimal should be equal to  $9/9 = 1$ .

It is also clear that the sum of the infinite series:

$$\frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \frac{9}{10000} + \dots$$

is 1, since from Equation 2 we obtain  $a = 9/10$  and  $r = 1/10$ , so  $a/(1 - r) = 1$ .

The ugly truth is that decimal expansions in our base-10 system are not unique. There are sometimes two different ways to represent the same fraction with different decimal expansions. There is nothing unique about the apparent problem that  $.999\dots = 1$ . The same thing occurs infinitely often:  $.3499999\dots = .35$ ,  $.11199999\dots = .112$ , et cetera.

This problem is not unique to base 10; if you are working in base 8, the number 1 has two ‘‘octal’’ expansions:  $1.0000\dots$  and  $0.7777\dots$ , et cetera.

## 6 What's with $1/81 = .012345679\dots$ ?

We will examine the title question later. Let us begin with a couple of easier examples.

We learned in Section 4 how to sum a geometric series and we can use that trick to make a couple of other interesting fractions. As the first example, consider the decimal expansion that begins like this:

$$D = .010204081632$$

If you look at each pair of digits, each is the double of the previous set of two. But we can also write it as a geometric series:

$$D = \frac{1}{100} + \frac{1}{100} \left(\frac{2}{100}\right)^1 + \frac{1}{100} \left(\frac{2}{100}\right)^2 + \frac{1}{100} \left(\frac{2}{100}\right)^3 + \dots$$

In this series the first term,  $a = 1/100$  and the ratio  $r = 2/100$ . Thus the sum should be:

$$D = \frac{a}{1-r} = \frac{1/100}{1-2/100} = \frac{1}{98}.$$

And sure enough, if we divide out  $1/98$ , we obtain:

$$\frac{1}{98} = .0102040816326530612244897959183673469387755$$

The doubling pattern seems to fail immediately after the 32: we have a 65 rather than a 64 in the pattern. But it's easy to see why, since the next term, 128, has more than two digits, so the 1 carries over into the next column to the left, turning 64 into 65.

You can go further with the following fraction:

$$\frac{1}{998} = .0010020040080160320641282565130260\dots$$

We've just written "... " since this one doesn't repeat for a while—its repeating cycle is 498 digits long.

Both the examples above are based on the fact that we know how to add up the terms in the geometric series:

$$S = a + ar + ar^2 + ar^3 + \dots = \frac{a}{1-r}. \quad (3)$$

The examples use values of  $r$  that have some power of 10 in the denominator and (usually) small integers in the numerator. If you understand this, it should be easy to find the fraction that corresponds to this decimal expansion:

$$.000100030009002700810243\dots,$$

where the numbers in the expansion start out looking like powers of 3.

But there are other series we know how to add. For example<sup>1</sup>:

$$r + 2r^2 + 3r^3 + 4r^4 + \dots = \frac{r}{(1-r)^2}. \quad (4)$$

---

<sup>1</sup>This formula can be obtained from the formula for the geometric series (Equation 3) by setting  $a = 1$  and then taking the derivative of both sides with respect to  $r$  and multiplying the result by  $r$ . We can begin with this result and do the same sort of thing to obtain Equation 5. But even without calculus, we can sum it. If  $S = r + r^2 + r^3 + \dots = r/(1-r)$ , then the sum in Equation 4 is equal to  $S + rS + r^2S + \dots = S(1 + r + r^2 + \dots) = S/(1-r) = r/(1-r)^2$ .

If  $r = 1/10$ , this formula gives:

$$.1 + .02 + .003 + \dots = .123\dots = 10/81.$$

If you divide by ten, you obtain  $1/81 = .012345679\dots$ . The decimal jumps from 7 to 9 because of carries that occur when the terms with 10 and above are added in.

Another way to see what is going on is to note that  $1/81 = 1/9 \cdot 1/9$ . We know the decimal expansion of  $1/9$ :  $1/9 = .11111\dots$ . Try using standard longhand multiplication of  $1/9$  by itself using the following decimal approximation: 0.1111111111. (It is not hard, and it makes the result obvious.)

More formulas like that above are not too hard to derive if you know a little calculus. For example:

$$r + 4r^2 + 9r^3 + 16r^4 + 25r^5 + \dots = \frac{r(1+r)}{(1-r)^3} \quad (5)$$

from which we can obtain:

$$\frac{100010000}{999700029999} = .000100040009001600250036\dots$$

As one final example, consider the Fibonacci numbers, defined as follows:  $F_0 = 0$ ,  $F_1 = 1$ ,  $F_n = F_{n-1} + F_{n-2}$ , if  $n > 1$ . The first few Fibonacci numbers are: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34,  $\dots$

$$\frac{1}{9899} = .00010102030508132134\dots$$

Can you find a fraction whose value is .000001001002003005 $\dots$ ?

Here are a couple of other fractions whose decimal expansions are interesting:  $1/97$  and  $1/243$ .

## 7 Cycle Lengths

In the rest of this paper, we will assume that the fractions we consider have been reduced to lowest terms. In other words, the numerator and denominator have no common factors. The fraction  $6/9$  is not reduced to lowest terms, since both 6 and 9 have a common factor of 3. The equivalent fraction  $2/3$  is reduced to lowest terms. This reduction is easy for small numerators and denominators, but it can be a bit messy with large numerators and denominators. There is a simple algorithm to reduce fractions, and it is explained in Appendix C.

A very interesting question is the following. Given a fraction  $p/q$  that is reduced to lowest terms, what is the length of the non-repeating part and what is the length of the cycle? Before reading on, you may wish to look at the data in the table in Appendix A and look for patterns. If you do see patterns, try to prove them.

We will show later that if  $p/q$  is reduced to lowest terms, it will have the same length non-repeating part and repeating part as  $1/q$ . You may wish to check this with a few examples, like  $1/7 = .\overline{142857}$ ,  $2/7 = .\overline{285714}$ ,  $3/7 = .\overline{428571}$ , et cetera. All have no non-repeating part and a repeating part of 6 digits.

Another example is  $1/6 = .\overline{16}$  and  $5/6 = .\overline{83}$ . Both have a single non-repeating digit followed by a single-digit repeating cycle.

We will prove this in Section 7.2, but this is the reason that the table in Appendix A only contains the data for fractions of the form  $1/N$ .

## 7.1 The Non-Repeating Part

The next thing to notice is the set of fractions in the list that terminate. It's clear that at least in the examples in Appendix A all and *only* those fractions with denominators of the form  $2^i 5^j$  terminate. This is related to the fact that we have ten fingers and therefore work in base  $10 = 2 \cdot 5$ . In fact, if you look at any terminating fraction with denominator  $2^i 5^j$ , the number of digits before the fraction terminates is exactly equal to the larger of  $i$  and  $j$ .

This should be clear, since any decimal that terminates in 1, 2, or 3 places has, by definition, a denominator of 10, 100, 1000, et cetera. So if we look, for example, at decimals that terminate after 3 places, the fraction has the form  $N/1000$  (or a reduced form of that), where  $N$  is a three-digit number. If  $N$  contains both a factor of 5 and of 2, we could divide numerator and denominator by 10 and make it terminate in 2 digits. Thus  $N$  may have factors of 2 or may have factors of 5, *but not both*.

Thus  $7/160 = 7/(2^5 \cdot 5)$  should terminate after exactly 5 terms, and it does:  $7/160 = .04375000\dots$

Now consider decimals with a repeating and a non-repeating part. Let's just consider an example, and it should be clear how to do a formal proof from the example. What is the fraction that has the expansion:  $.217\overline{6543}$ ? Write it like this:

$$.217\overline{6543} = \frac{217}{1000} + \frac{1}{1000} \cdot \frac{6543}{9999}.$$

In this case it's obvious that there will be a denominator of the final fraction with at least three 2s or three 5s. But with an appropriate selection of non-repeating and cycle parts, could we have some cancellation? For example, how about  $.250\overline{750}$ ? This would be:

$$.250\overline{750} = \frac{250}{1000} + \frac{1}{1000} \cdot \frac{750}{999}.$$

We can divide 10 out of the numerator and denominator of both parts, and only have a fraction of 100, guaranteeing a non-repeating part of only two digits. What's wrong?

Well, here's what's wrong: we did not write the original decimal in its simplest form:

$$.250\overline{750} = .25\overline{075},$$

so it really has only a two-digit non-repeating part.

In any case, with a little thought it should be clear that any decimal that repeats after an initial non-repeating part of  $k$  digits must contain at least  $2^k$  or  $5^k$  in the denominator, and no powers of 2 or 5 greater than  $k$ .

There is an easy way to convert fractions that have a non-repeating as well as a repeating part. We will leave it as an exercise for you to discover the exact rule and proof of the rule, but look at the following conversions, and find the underlying pattern:

$$\begin{aligned} .1\overline{37} &= (137 - 1)/990 = 136/990 \\ .123\overline{72} &= (12372 - 123)/99000 = 12249/99000 \\ .123\overline{5} &= (1235 - 123)/9000 = 1112/9000 \\ .134\overline{72} &= (13472 - 13)/99900 = 13459/99900 \\ .11235\overline{7166} &= (112357166 - 1123)/999990000 = 112356043/999990000. \end{aligned}$$

## 7.2 Repeating Cycle Length

If we look over a bunch of examples in Appendix A, we can find still more patterns. Since we know how to deal with factors of 2 and 5 in the denominators, let's ignore those and look only at denominators that are products of prime numbers other than 2 and 5. Here are a few interesting patterns:



Consider the  $n$  distinct remainders  $1 = r_0, r_1, \dots, r_{n-1}$ , where  $r_n = r_0 = 1$  obtained during the long division of  $1/N$ . If  $n = N - 1$  then all the remainders from 1 to  $N - 1$  must appear somewhere in the cycle, so the long division of  $k/N$  will simply begin in the cycle at the point where  $r_i = k$  and continue with exactly the same cycle elements around a cycle of exactly the same length  $n = N - 1$ .

If  $n < N - 1$  then some of the remainders are omitted. If  $m$  is an omitted remainder and  $m/N$  is reduced to lowest terms, then in the long division of  $m/N$ , we must obtain remainders  $mr_0, mr_1, mr_2, \dots, mr_{n-1}$ , all taken mod  $N$ . Clearly the cycle repeats at this point, since  $mr_n = m \pmod N$ . It cannot repeat earlier. If it did, and  $mr_0 = mr_j$  for  $j < n - 1$ , then  $r_0 = r_j \pmod N$  because  $\text{GCD}(m, N) = 1$ . This cannot occur since  $r_{n-1}$  is the first time the remainders  $r_j$  return to  $1 \pmod N$ . Thus every irreducible fraction  $k/N$  has the same cycle length as the fraction  $1/N$ .

Finally, note that if  $N$  is prime, all the fractions  $k/N$  are irreducible, so all the remainders fall into equivalence classes determined by which cycle they are in. But all these cycles have the same length, so the cycle lengths must divide  $N - 1$ . This is only true if  $N$  is prime, however. The cycle length of  $1/14$ , for example, is 6, which does not divide 13.

### 7.3 The General Problem

In general, what we would like to do is given a reduced fraction  $k/n$ , find the length of the non-repeating and repeating part of its decimal expansion. In the examples below, the primes we consider do not include 2 and 5.

We know how to find the non-repeating length: if  $2^i$  and  $5^j$  are the largest powers of 2 and 5 that divide  $n$ , then the non-repeating part has a length which is the maximum of  $i$  and  $j$ . Unfortunately, nobody knows an easy way to find the length of the repeating part, even when  $n$  is a prime number.

Here are some partial results, where we'll assume that the denominator of  $k/n$  is not divisible by 2 or 5, and that  $k/n$  is reduced to lowest terms. In what follows, we'll denote by  $\lambda(n)$  the length of the cycle of the fraction  $k/n$ .

1.  $\lambda(n) = i$  if  $i > 0$  is the smallest integer such that  $10^i = 1 \pmod n$ .
2. If  $p$  is a prime, that  $0 < k < p$ , and the cycle length of  $k/p$  is even, then if the first half of the cycle is added to the last half as integers, the result is  $10^{\lambda(p)/2} - 1$ . For example,  $1/7 = .\overline{142857}$ , and  $142 + 857 = 999 = 10^3 - 1$ . Another example:  $1/17 = .\overline{0588235294117647}$ , and  $05882352 + 94117647 = 99999999 = 10^8 - 1$ .

To show this, assume that the cycle length is  $2m$ , where  $m$  is an integer. Since the cycle length is  $2m$  that means that  $10^{2m} = 1 \pmod p$ . Then the decimal representation of  $k/p$  is:

$$\frac{k}{p} = .d_1 d_2 \dots d_{2m} d_1 d_2 \dots d_{2m} d_1 d_2 \dots$$

Then

$$10^m \frac{k}{p} = d_1 d_2 \dots d_m + .d_{m+1} d_{m+2} \dots d_{2m} d_1 d_2 \dots d_{2m} d_1 d_2 \dots,$$

where  $N = d_1 d_2 \dots d_m$  is a whole number. If we add the two expressions above, we obtain:

$$(10^m + 1) \frac{k}{p} = N + .e_1 e_2 \dots e_{2m} e_1 e_2 \dots e_{2m} e_1 e_2 \dots,$$

where the  $e_i$  are the decimal digits obtained by adding the first and last halves of the digits in the decimal expansion of  $k/p$ . If all the  $e_i$  are equal to 9 then the sum on the right is a whole number as well.

This will be true if  $(10^m + 1)$  is a multiple of  $p$ . But we know that  $10^{2m} = 1 \pmod{p}$ , so  $10^{2m} - 1 = (10^m + 1)(10^m - 1) = 0 \pmod{p}$ . So  $p$  must divide  $(10^m + 1)$  or  $(10^m - 1)$ . Note that  $(10^m - 1)$  is a series of 9's, and if  $p$  divided that, there would be a decimal representation of  $k/p$  with half the repeat length. Thus  $p$  divides  $(10^m + 1)$  and we are done.

3. If  $p$  is prime, then the length of the cycle divides  $p - 1$ .

Suppose that the cycle length is  $m$ . Then  $m$  is the smallest positive integer such that  $10^m = 1 \pmod{p}$ . If  $k$  is any integer such that  $10^k = 1 \pmod{p}$  then  $k$  must be a multiple of  $m$ . Fermat's little theorem tells us that  $10^{p-1} = 1 \pmod{p}$ , so  $m$  must divide  $p - 1$ .

4. If 10 is a primitive root of  $n$ , then  $\lambda(n) = \phi(n)$ , where  $\phi$  is the Euler totient function. See Appendix D for properties of the totient function, and Appendix E for the properties of primitive roots. For example, 10 is a primitive root mod 49 and  $\phi(49) = 42$  so the cycle length of  $1/49$  is 42.

5.  $\lambda(n)$  divides  $\phi(n)$ .

## 8 Cyclic Numbers

This section is not really about fractions and decimals, but as you will see, it is closely related.

A cyclic number is an integer of length  $n$  such that if you multiply it by all the numbers from 1 to  $n - 1$  you get the same sequence of numbers, but rotated by some amount. (This definition can be made in any base, but we will stick to base-10 here. Also, we will allow the  $n$ -digit number to begin with any number of zeroes, except for all of them.)

The simplest non-trivial cyclic number is 142857:

$$\begin{aligned} 1 \times 142857 &= 142857 \\ 2 \times 142857 &= 285714 \\ 3 \times 142857 &= 428571 \\ 4 \times 142857 &= 571428 \\ 5 \times 142857 &= 714285 \\ 6 \times 142857 &= 857142 \end{aligned}$$

The number 142857 is the repeating part of the decimal expansion of  $1/7$ . It turns out that if  $p$  is a prime number other than 2 or 5, and if the repeating part of the decimal expansion of  $1/p$  has  $p - 1$  digits, then that repeating part, expressed as an integer, will be a cyclic number.

It turns out that the only way to get a cyclic number is if it has length  $p - 1$ , where  $p$  is some prime number. Not all primes work, however. Consider  $p = 13$ :

$$\begin{array}{ll} 1 \times 076923 &= 076923 & 7 \times 076923 &= 538461 \\ 2 \times 076923 &= 153846 & 8 \times 076923 &= 615384 \\ 3 \times 076923 &= 230769 & 9 \times 076923 &= 692307 \\ 4 \times 076923 &= 307692 & 10 \times 076923 &= 769230 \\ 5 \times 076923 &= 384615 & 11 \times 076923 &= 846153 \\ 6 \times 076923 &= 461538 & 12 \times 076923 &= 923076 \end{array}$$

Here there are two 6-digit sequences, all of whose rotations appear. In general, this is what will happen: the length of the repeating sequence will divide  $p - 1$  and it will form a cyclic number only if its length is exactly  $p - 1$ .

This will happen exactly when all the remainders of  $(10^i \bmod p)$  are different for  $1 \leq i \leq p - 1$ . This is easy to see, since dividing  $p$  into  $10^k$  is effectively what we are doing when we do long division.

Let's look at  $1/17$  whose repeating part is 0588235294117647.

$$\begin{array}{llll}
 1 \times 0588235294117647 & = & 0588235294117647 & 9 \times 0588235294117647 & = & 5294117647058823 \\
 2 \times 0588235294117647 & = & 1176470588235294 & 10 \times 0588235294117647 & = & 5882352941176470 \\
 3 \times 0588235294117647 & = & 1764705882352941 & 11 \times 0588235294117647 & = & 6470588235294117 \\
 4 \times 0588235294117647 & = & 2352941176470588 & 12 \times 0588235294117647 & = & 7058823529411764 \\
 5 \times 0588235294117647 & = & 2941176470588235 & 13 \times 0588235294117647 & = & 7647058823529411 \\
 6 \times 0588235294117647 & = & 3529411764705882 & 14 \times 0588235294117647 & = & 8235294117647058 \\
 7 \times 0588235294117647 & = & 4117647058823529 & 15 \times 0588235294117647 & = & 8823529411764705 \\
 8 \times 0588235294117647 & = & 4705882352941176 & 16 \times 0588235294117647 & = & 9411764705882352
 \end{array}$$

This does form the longest possible cycle.

Here is one more thing to notice which should be obvious if we consider what we have already learned about decimal expansions:

$$\begin{array}{ll}
 7 \times 142857 & = & 999999 \\
 13 \times 076923 & = & 999999 \\
 17 \times 0588235294117647 & = & 9999999999999999
 \end{array}$$

## 8.1 Artin's Conjecture

Some primes  $p$  work (can be used to make a cyclic number) and some don't here are the first few primes that work:

$$7, 17, 19, 23, 29, 47, 59, 61, 97, 109.$$

What proportion of the primes have this property? The answer is that nobody knows, and in fact, there may only be a finite number of cyclic numbers. However there is a lot of empirical evidence that there are an infinite number and, in fact, that the proportion of primes that generate a cyclic number is, in the limit, 0.3739558136... or about thirty seven percent. This is a pretty big gap between evidence and conjecture. The evidence indicates that these numbers are very common, but on the other hand, there may be only a fixed number of them. That this limit holds is called "Artin's Conjecture."

## 8.2 Midy's Theorem

We noticed earlier that if we have a cyclic number of length  $p - 1$  that if we divide it into two halves and add them together, we get a number made of all 9's. For  $p = 7$  the cyclic number is 142857. Add the half numbers:  $142 + 857 = 999$ . For  $p = 17$ : 0588235294117647 becomes  $05882352 + 94117647 = 99999999$ .

But look at this:

$$14 + 28 + 57 = 99.$$

Or this:

$$0588 + 2352 + 9411 + 7647 = 19998 = 2 \times 9999.$$

Or this:

$$05 + 88 + 23 + 52 + 94 + 11 + 76 + 47 = 396 = 4 \times 99.$$

Midy's theorem states that if we have a cyclic number generated by a prime  $p$ , then if  $k$  divides  $p - 1$ , we can divide the number into groups of digits that are  $(p - 1)/k$  long and we will obtain a number that is an integer multiple of the number made of a series of  $(p - 1)/k$  copies of 9.

## 9 Other Bases

Everything in this document has been calculated in base-10. Similar things can be said if we are using other bases. We won't do much here except to show what the situation looks like in another base: base-7. In what follows, we will indicate numbers written in base-7 with a subscript of 7. Thus,  $23 = 32_7$  means 23 in base-10 is the same as 32 in base-7.

Seven is prime, so with this base, the only fractions that come out "even" are those whose denominator is a power of 7. (In base-10 fractions with denominators which are a product of powers of 2 and 5 come out even.)

Similarly, if the denominator is a product of  $7^k$  and other primes, the expansion will have  $k$  digits followed by the repeating part.

Here are some expansions of fractions in base-7. Note that the fractions and the expansions are in base-7.

$1/2_7$	$.\overline{3}_7$	$1/15_7$	$.\overline{04}_7$	$1/31_7$	$.\overline{0214064526}_7$
$1/3_7$	$.\overline{2}_7$	$1/16_7$	$.\overline{035245631421}_7$	$1/32_7$	$.\overline{0206251134364604155323}_7$
$1/4_7$	$.\overline{15}_7$	$1/20_7$	$.\overline{03}_7$	$1/33_7$	$.\overline{02}_7$
$1/5_7$	$.\overline{1254}_7$	$1/21_7$	$.\overline{0316}_7$	$1/34_7$	$.\overline{0165}_7$
$1/6_7$	$.\overline{1}_7$	$1/22_7$	$.\overline{03}_7$	$1/35_7$	$.\overline{016122650544}_7$
$1/10_7$	$.1_7$	$1/23_7$	$.\overline{0261143464055232}_7$	$1/36_7$	$.\overline{15463241015463241}_7$
$1/11_7$	$.\overline{06}_7$	$1/24_7$	$.\overline{025}_7$	$1/40_7$	$.\overline{015}_7$
$1/12_7$	$.\overline{053}_7$	$1/25_7$	$.\overline{024}_7$	$1/41_7$	$.\overline{0145536}_7$
$1/13_7$	$.\overline{0462}_7$	$1/26_7$	$.\overline{0231}_7$	$1/42_7$	$.\overline{0143}_7$
$1/14_7$	$.\overline{0431162355}_7$	$1/30_7$	$.\overline{02}_7$	$1/43_7$	$.\overline{014031062154342}_7$

Referring to the previous section, we can see the repeating parts of the following expansions of numbers are cyclic in base-7:

$$1/5_7, 1/14_7, 1/16_7, 1/23_7, 1/32_7,$$

so the first few cyclic numbers in base-7 are:

$$1254_7, 0431162355_7, 035245631421_7, 0261143464055232_7, 0206251134364604155323_7.$$

We can show that Midy's theorem also seems to hold in this base using  $035245631421_7$ :

$$\begin{aligned} 035245_7 + 631421_7 &= 666666_7 \\ 0352_7 + 4563_7 + 1421_7 &= 6666_7 \\ 035_7 + 245_7 + 631_7 + 421_7 &= 1665_7 = 2 \times 666_7 \\ 03_7 + 52_7 + 45_7 + 63_7 + 14_7 + 21_7 &= 264_7 = 3 \times 66_7. \end{aligned}$$

## A Cycle Length Table for 1/1 to 1/900

Pattern: ||Denominator|Non-repeat|Repeat||. Example:  $1/12 = .08333\dots$ . Denominator is 12, the “08” does not repeat, length is 2, the “3” repeats, length is 1. “•” signifies a terminating decimal.

1	0	•	51	0	16	101	0	4	151	0	75	201	0	33	251	0	50
2	1	•	52	2	6	102	1	16	152	3	18	202	1	4	252	2	6
3	0	1	53	0	13	103	0	34	153	0	16	203	0	84	253	0	22
4	2	•	54	1	3	104	3	6	154	1	6	204	2	16	254	1	42
5	1	•	55	1	2	105	1	6	155	1	15	205	1	5	255	1	16
6	1	1	56	3	6	106	1	13	156	2	6	206	1	34	256	8	•
7	0	6	57	0	18	107	0	53	157	0	78	207	0	22	257	0	256
8	3	•	58	1	28	108	2	3	158	1	13	208	4	6	258	1	21
9	0	1	59	0	58	109	0	108	159	0	13	209	0	18	259	0	6
10	1	•	60	2	1	110	1	2	160	5	•	210	1	6	260	2	6
11	0	2	61	0	60	111	0	3	161	0	66	211	0	30	261	0	28
12	2	1	62	1	15	112	4	6	162	1	9	212	2	13	262	1	130
13	0	6	63	0	6	113	0	112	163	0	81	213	0	35	263	0	262
14	1	6	64	6	•	114	1	18	164	2	5	214	1	53	264	3	2
15	1	1	65	1	6	115	1	22	165	1	2	215	1	21	265	1	13
16	4	•	66	1	2	116	2	28	166	1	41	216	3	3	266	1	18
17	0	16	67	0	33	117	0	6	167	0	166	217	0	30	267	0	44
18	1	1	68	2	16	118	1	58	168	3	6	218	1	108	268	2	33
19	0	18	69	0	22	119	0	48	169	0	78	219	0	8	269	0	268
20	2	•	70	1	6	120	3	1	170	1	16	220	2	2	270	1	3
21	0	6	71	0	35	121	0	22	171	0	18	221	0	48	271	0	5
22	1	2	72	3	1	122	1	60	172	2	21	222	1	3	272	4	16
23	0	22	73	0	8	123	0	5	173	0	43	223	0	222	273	0	6
24	3	1	74	1	3	124	2	15	174	1	28	224	5	6	274	1	8
25	2	•	75	2	1	125	3	•	175	2	6	225	2	1	275	2	2
26	1	6	76	2	18	126	1	6	176	4	2	226	1	112	276	2	22
27	0	3	77	0	6	127	0	42	177	0	58	227	0	113	277	0	69
28	2	6	78	1	6	128	7	•	178	1	44	228	2	18	278	1	46
29	0	28	79	0	13	129	0	21	179	0	178	229	0	228	279	0	15
30	1	1	80	4	•	130	1	6	180	2	1	230	1	22	280	3	6
31	0	15	81	0	9	131	0	130	181	0	180	231	0	6	281	0	28
32	5	•	82	1	5	132	2	2	182	1	6	232	3	28	282	1	46
33	0	2	83	0	41	133	0	18	183	0	60	233	0	232	283	0	141
34	1	16	84	2	6	134	1	33	184	3	22	234	1	6	284	2	35
35	1	6	85	1	16	135	1	3	185	1	3	235	1	46	285	1	18
36	2	1	86	1	21	136	3	16	186	1	15	236	2	58	286	1	6
37	0	3	87	0	28	137	0	8	187	0	16	237	0	13	287	0	30
38	1	18	88	3	2	138	1	22	188	2	46	238	1	48	288	5	1
39	0	6	89	0	44	139	0	46	189	0	6	239	0	7	289	0	272
40	3	•	90	1	1	140	2	6	190	1	18	240	4	1	290	1	28
41	0	5	91	0	6	141	0	46	191	0	95	241	0	30	291	0	96
42	1	6	92	2	22	142	1	35	192	6	1	242	1	22	292	2	8
43	0	21	93	0	15	143	0	6	193	0	192	243	0	27	293	0	146
44	2	2	94	1	46	144	4	1	194	1	96	244	2	60	294	1	42
45	1	1	95	1	18	145	1	28	195	1	6	245	1	42	295	1	58
46	1	22	96	5	1	146	1	8	196	2	42	246	1	5	296	3	3
47	0	46	97	0	96	147	0	42	197	0	98	247	0	18	297	0	6
48	4	1	98	1	42	148	2	3	198	1	2	248	3	15	298	1	148
49	0	42	99	0	2	149	0	148	199	0	99	249	0	41	299	0	66
50	2	•	100	2	•	150	2	1	200	3	•	250	3	•	300	2	1

301	0	42	351	0	6	401	0	200	451	0	10	501	0	166	551	0	252
302	1	75	352	5	2	402	1	33	452	2	112	502	1	50	552	3	22
303	0	4	353	0	32	403	0	30	453	0	75	503	0	502	553	0	78
304	4	18	354	1	58	404	2	4	454	1	113	504	3	6	554	1	69
305	1	60	355	1	35	405	1	9	455	1	6	505	1	4	555	1	3
306	1	16	356	2	44	406	1	84	456	3	18	506	1	22	556	2	46
307	0	153	357	0	48	407	0	6	457	0	152	507	0	78	557	0	278
308	2	6	358	1	178	408	3	16	458	1	228	508	2	42	558	1	15
309	0	34	359	0	179	409	0	204	459	0	48	509	0	508	559	0	42
310	1	15	360	3	1	410	1	5	460	2	22	510	1	16	560	4	6
311	0	155	361	0	342	411	0	8	461	0	460	511	0	24	561	0	16
312	3	6	362	1	180	412	2	34	462	1	6	512	9	●	562	1	28
313	0	312	363	0	22	413	0	174	463	0	154	513	0	18	563	0	281
314	1	78	364	2	6	414	1	22	464	4	28	514	1	256	564	2	46
315	1	6	365	1	8	415	1	41	465	1	15	515	1	34	565	1	112
316	2	13	366	1	60	416	5	6	466	1	232	516	2	21	566	1	141
317	0	79	367	0	366	417	0	46	467	0	233	517	0	46	567	0	18
318	1	13	368	4	22	418	1	18	468	2	6	518	1	6	568	3	35
319	0	28	369	0	5	419	0	418	469	0	66	519	0	43	569	0	284
320	6	●	370	1	3	420	2	6	470	1	46	520	3	6	570	1	18
321	0	53	371	0	78	421	0	140	471	0	78	521	0	52	571	0	570
322	1	66	372	2	15	422	1	30	472	3	58	522	1	28	572	2	6
323	0	144	373	0	186	423	0	46	473	0	42	523	0	261	573	0	95
324	2	9	374	1	16	424	3	13	474	1	13	524	2	130	574	1	30
325	2	6	375	3	1	425	2	16	475	2	18	525	2	6	575	2	22
326	1	81	376	3	46	426	1	35	476	2	48	526	1	262	576	6	1
327	0	108	377	0	84	427	0	60	477	0	13	527	0	240	577	0	576
328	3	5	378	1	6	428	2	53	478	1	7	528	4	2	578	1	272
329	0	138	379	0	378	429	0	6	479	0	239	529	0	506	579	0	192
330	1	2	380	2	18	430	1	21	480	5	1	530	1	13	580	2	28
331	0	110	381	0	42	431	0	215	481	0	6	531	0	58	581	0	246
332	2	41	382	1	95	432	4	3	482	1	30	532	2	18	582	1	96
333	0	3	383	0	382	433	0	432	483	0	66	533	0	30	583	0	26
334	1	166	384	7	1	434	1	30	484	2	22	534	1	44	584	3	8
335	1	33	385	1	6	435	1	28	485	1	96	535	1	53	585	1	6
336	4	6	386	1	192	436	2	108	486	1	27	536	3	33	586	1	146
337	0	336	387	0	21	437	0	198	487	0	486	537	0	178	587	0	293
338	1	78	388	2	96	438	1	8	488	3	60	538	1	268	588	2	42
339	0	112	389	0	388	439	0	219	489	0	81	539	0	42	589	0	90
340	2	16	390	1	6	440	3	2	490	1	42	540	2	3	590	1	58
341	0	30	391	0	176	441	0	42	491	0	490	541	0	540	591	0	98
342	1	18	392	3	42	442	1	48	492	2	5	542	1	5	592	4	3
343	0	294	393	0	130	443	0	221	493	0	112	543	0	180	593	0	592
344	3	21	394	1	98	444	2	3	494	1	18	544	5	16	594	1	6
345	1	22	395	1	13	445	1	44	495	1	2	545	1	108	595	1	48
346	1	43	396	2	2	446	1	222	496	4	15	546	1	6	596	2	148
347	0	173	397	0	99	447	0	148	497	0	210	547	0	91	597	0	99
348	2	28	398	1	99	448	6	6	498	1	41	548	2	8	598	1	66
349	0	116	399	0	18	449	0	32	499	0	498	549	0	60	599	0	299
350	2	6	400	4	●	450	2	1	500	3	●	550	2	2	600	3	1

601	0	300	651	0	30	701	0	700	751	0	125	801	0	44	851	0	66
602	1	42	652	2	81	702	1	6	752	4	46	802	1	200	852	2	35
603	0	33	653	0	326	703	0	18	753	0	50	803	0	8	853	0	213
604	2	75	654	1	108	704	6	2	754	1	84	804	2	33	854	1	60
605	1	22	655	1	130	705	1	46	755	1	75	805	1	66	855	1	18
606	1	4	656	4	5	706	1	32	756	2	6	806	1	30	856	3	53
607	0	202	657	0	8	707	0	12	757	0	27	807	0	268	857	0	856
608	5	18	658	1	138	708	2	58	758	1	378	808	3	4	858	1	6
609	0	84	659	0	658	709	0	708	759	0	22	809	0	202	859	0	26
610	1	60	660	2	2	710	1	35	760	3	18	810	1	9	860	2	21
611	0	138	661	0	220	711	0	13	761	0	380	811	0	810	861	0	30
612	2	16	662	1	110	712	3	44	762	1	42	812	2	84	862	1	215
613	0	51	663	0	48	713	0	330	763	0	108	813	0	5	863	0	862
614	1	153	664	3	41	714	1	48	764	2	95	814	1	6	864	5	3
615	1	5	665	1	18	715	1	6	765	1	16	815	1	81	865	1	43
616	3	6	666	1	3	716	2	178	766	1	382	816	4	16	866	1	432
617	0	88	667	0	308	717	0	7	767	0	174	817	0	126	867	0	272
618	1	34	668	2	166	718	1	179	768	8	1	818	1	204	868	2	30
619	0	618	669	0	222	719	0	359	769	0	192	819	0	6	869	0	26
620	2	15	670	1	33	720	4	1	770	1	6	820	2	5	870	1	28
621	0	66	671	0	60	721	0	102	771	0	256	821	0	820	871	0	66
622	1	155	672	5	6	722	1	342	772	2	192	822	1	8	872	3	108
623	0	132	673	0	224	723	0	30	773	0	193	823	0	822	873	0	96
624	4	6	674	1	336	724	2	180	774	1	21	824	3	34	874	1	198
625	4	•	675	2	3	725	2	28	775	2	15	825	2	2	875	3	6
626	1	312	676	2	78	726	1	22	776	3	96	826	1	174	876	2	8
627	0	18	677	0	338	727	0	726	777	0	6	827	0	413	877	0	438
628	2	78	678	1	112	728	3	6	778	1	388	828	2	22	878	1	219
629	0	48	679	0	96	729	0	81	779	0	90	829	0	276	879	0	146
630	1	6	680	3	16	730	1	8	780	2	6	830	1	41	880	4	2
631	0	315	681	0	113	731	0	336	781	0	70	831	0	69	881	0	440
632	3	13	682	1	30	732	2	60	782	1	176	832	6	6	882	1	42
633	0	30	683	0	341	733	0	61	783	0	84	833	0	336	883	0	441
634	1	79	684	2	18	734	1	366	784	4	42	834	1	46	884	2	48
635	1	42	685	1	8	735	1	42	785	1	78	835	1	166	885	1	58
636	2	13	686	1	294	736	5	22	786	1	130	836	2	18	886	1	221
637	0	42	687	0	228	737	0	66	787	0	393	837	0	15	887	0	886
638	1	28	688	4	21	738	1	5	788	2	98	838	1	418	888	3	3
639	0	35	689	0	78	739	0	246	789	0	262	839	0	419	889	0	42
640	7	•	690	1	22	740	2	3	790	1	13	840	3	6	890	1	44
641	0	32	691	0	230	741	0	18	791	0	336	841	0	812	891	0	18
642	1	53	692	2	43	742	1	78	792	3	2	842	1	140	892	2	222
643	0	107	693	0	6	743	0	742	793	0	60	843	0	28	893	0	414
644	2	66	694	1	173	744	3	15	794	1	99	844	2	30	894	1	148
645	1	21	695	1	46	745	1	148	795	1	13	845	1	78	895	1	178
646	1	144	696	3	28	746	1	186	796	2	99	846	1	46	896	7	6
647	0	646	697	0	80	747	0	41	797	0	199	847	0	66	897	0	66
648	3	9	698	1	116	748	2	16	798	1	18	848	4	13	898	1	32
649	0	58	699	0	232	749	0	318	799	0	368	849	0	141	899	0	420
650	2	6	700	2	6	750	3	1	800	5	•	850	2	16	900	2	1

## B The mod Function

In this appendix, we assume that we are dealing only with integers, although the concept is easy to extend to real numbers in some cases. The definition of  $m \bmod n$  is the remainder obtained if  $m$  is divided by  $n$ . Thus  $5 \bmod 3 = 2$ ,  $15 \bmod 5 = 0$ , and  $17 \bmod 20 = 17$ . The value of  $m \bmod n$  is always between 0 and  $n - 1$ , inclusive.

We sometimes write  $m \equiv n \pmod{k}$  to mean  $m \bmod k = n \bmod k$ . In English, we say that “ $m$  is equivalent to  $n$ , mod  $k$ ”. In this case the “mod” is a congruence relation.

Here are some easily proved properties of the mod congruence relation. Some of them involve the function *GCD*, or “greatest common divisor” that is dealt with in Appendix C

$$\begin{array}{llll}
 a \equiv b \pmod{n} & \text{and} & c \equiv d \pmod{n} & \implies & a + c \equiv b + d \pmod{n} \\
 a \equiv b \pmod{n} & \text{and} & c \equiv d \pmod{n} & \implies & a - c \equiv b - d \pmod{n} \\
 a \equiv b \pmod{n} & \text{and} & c \equiv d \pmod{n} & \implies & ac \equiv bd \pmod{n} \\
 a \equiv b \pmod{n} & \text{and} & m \geq 0 & \implies & a^m \equiv b^m \pmod{n} \\
 ac \equiv bc \pmod{n} & \text{and} & \text{GCD}(c, n) = 0 & \implies & a \equiv b \pmod{n} \\
 ac \equiv bc \pmod{nc} & \text{and} & c \neq 0 & \implies & a \equiv b \pmod{n} \\
 a \equiv b \pmod{mn} & \text{and} & \text{GCD}(m, n) = 0 & \implies & a \equiv b \pmod{m} \text{ and } a \equiv b \pmod{n}
 \end{array}$$

## C The GCD and Reducing Fractions

If you are given a fraction in the form  $m/n$ , where  $m$  and  $n$  are integers, it is usually far easier to work with if it is reduced to lowest terms. For example,  $1/2 = 2/4 = 3/6 = 4/8$ , but the form  $1/2$  is usually best, especially for the sorts of analyses done in this paper.

To reduce the fraction  $m/n$  to lowest terms, you need to find the largest integer  $r$  such that  $m = pr$  and  $n = qr$  where  $p$  and  $q$  are integers. Then  $m/n = pr/qr = p/q$ , and  $p/q$  is the reduced form of  $m/n$ .

The value  $r$  in the previous paragraph is called the “greatest common divisor” or “*GCD*” of  $m$  and  $n$ . Here is how to calculate the *GCD* for  $m, n \geq 0$ :

$$\text{GCD}(m, n) = \begin{cases} n & : m = 0 \\ \text{GCD}(n \bmod m, m) & : m > 0 \end{cases}$$

where  $n \bmod m$  is the remainder after dividing  $n$  by  $m$ . This recursive formula can be applied to calculate relatively quickly the *GCD* of any pair of numbers.

For example, let us find the *GCD*(197715, 22820):

$$\begin{aligned}
 \text{GCD}(197715, 22820) &= \text{GCD}(197715 \bmod 22820, 22820) \\
 &= \text{GCD}(15155, 22820) = \text{GCD}(22820 \bmod 15155, 15155) \\
 &= \text{GCD}(7665, 15155) = \text{GCD}(15155 \bmod 15155, 7665) \\
 &= \text{GCD}(7490, 7665) = \text{GCD}(7665 \bmod 7490, 7490) \\
 &= \text{GCD}(175, 7490) = \text{GCD}(7490 \bmod 175, 175) \\
 &= \text{GCD}(140, 175) = \text{GCD}(175 \bmod 140, 140) \\
 &= \text{GCD}(35, 140) = \text{GCD}(140 \bmod 35, 35) \\
 &= \text{GCD}(0, 35) = 35
 \end{aligned}$$

Thus the fraction  $22820/197715$  reduced to lowest terms is  $(22820/35)/(197715/35) = 652/5649$ . Usually the *GCD* operation does not require so many steps, but the example above illustrates how it will

grind down any two numbers, no matter how large.

## D The Euler Totient Function

The function  $\phi(n)$  is equal to the number of integers in the set  $\{1, 2, \dots, n-1\}$  that are relatively prime to  $n$ .  $\phi(1) = 1$ ,  $\phi(2) = 1$ ,  $\phi(3) = 2$ , and so on.

Here are values of  $\phi(n)$  for  $n = 1, 2, \dots, 50$ : 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8, 12, 10, 22, 8, 20, 12, 18, 12, 28, 8, 30, 16, 20, 16, 24, 12, 36, 18, 24, 16, 40, 12, 42, 20, 24, 22, 46, 16, 42, 20.

Obviously, if  $p$  is prime,  $\phi(p) = p - 1$  and  $\phi(p^k) = p^{k-1}(p - 1) = p^k(1 - 1/p)$ . If  $m$  is composite,  $\phi(m) < m - 1$ .

In general, if the prime factorization for an integer  $n$  is given by  $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ , then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

## E Primitive Roots mod $n$

If  $n$  is an integer then  $k$  is a primitive root mod  $n$  if  $k$  is relatively prime to  $n$ , if  $k^1, k^2, \dots, k^i = 1 \pmod n$  are all distinct, and  $i = \phi(n)$ .

For example, 3 is a primitive root mod  $n$  since  $3^1 = 3$ ,  $3^2 = 9$ ,  $3^3 = 7$  and  $3^4 = 1$ , all mod  $n$ , and in addition,  $\phi(10) = 4$ . There are no primitive roots mod 12. The only possibilities are in the set of numbers relatively prime to 12:  $\{1, 5, 7, 11\}$ .  $\phi(12) = 4$ , and  $1^2 = 5^2 = 7^2 = 11^2 = 1 \pmod{12}$ .

Here is a list of the first few integers that have a primitive root: 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27, 29.